

SafePatch for Windows Version 1.0 User Manual

D. Lim, T. Meier

U.S. Department of Energy

Lawrence
Livermore
National
Laboratory

May 1, 2003



SafePatch for Windows

Version 1.0

User Manual

May 2003

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This report has been reproduced
directly from the best available copy.

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information
P.O. Box 62, Oak Ridge, TN 37831
Prices available from (423) 576-8401, FTS 626-8401.

Available to the public from the
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd.
Springfield, VA 22161

This work was performed under the auspices of the U.S. Department of Energy by University of California Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48.

TABLE OF CONTENTS

1. WHAT IS SAFEPATCH FOR WINDOWS?	1
1.1 JOBS PANEL	1
1.2 TARGETS PANEL.....	1
1.3 EVALUATIONS PANEL	1
1.4 PATCHES PANEL.....	1
1.5 PACKAGED UPDATES PANEL	1
1.6 SETTINGS PANEL	1
2. GETTING STARTED.....	2
2.1 INSTALLING SAFEPATCH FOR WINDOWS.....	2
2.3 STARTING SAFEPATCH FOR WINDOWS.....	4
2.4 CREATING A HOST JOB TO GET THE LATEST EVALUATION DATABASE	5
2.5 ADDING TARGETS	6
2.6 CREATING A TARGET JOB	7
2.7 VIEWING THE PACKAGED UPDATES (INSTALLATION PACKAGES)	8
3 JOBS PANEL	9
3.1 TARGET JOB PANEL.....	10
3.2 HOST JOB PANEL	11
3.3 JOB PROPERTIES PANEL	12
3.4 DELETE JOB.....	12
4 TARGETS PANEL.....	13
5 EVALUATIONS PANEL.....	15
6 PATCHES PANEL.....	17
6.1 LOCAL PATCH DB	18
6.2 KNOWLEDGE BASE.....	18
6.3 COLLECTION RESULTS.....	19
7 PACKAGED UPDATES PANEL	20
8 SETTINGS PANEL.....	22
9 INTERPRETING THE SAFEPATCH EVALUATION RESULTS	24
APPENDIX A GLOSSARY	25
APPENDIX B ADMINISTRATOR PRIVILEGES.....	26
APPENDIX C SAFEPATCH COMMAND LINE.....	29
APPENDIX D TROUBLESHOOTING.....	30
D.1 VERIFY EVALUATION TOOL EXISTS	30
D.2 ERROR CREATING THE TARGET PACKAGE.....	31
D.3 *** SECOND INSTANCE OF SAFEPATCH NOT ALLOWED ***	33
D.4 THE SAFEPATCH USER INTERFACE IS NOT RESPONDING	33

D.5 THE PATCHES DO NOT SEEM TO BE INSTALLING	34
APPENDIX E SUPPORT UTILITIES	35
<i>Using Wget.exe</i>	35
<i>Using Qchain.exe</i>	35
<i>Using Extract.exe</i>	35
<i>Using HFNetChk.exe</i>	35
Scanning Pre-Requisites	36
<i>Using Mbsaccli.exe</i>	36
APPENDIX F PATCH INFORMATION	37

1. What is SafePatch for Windows?

SafePatch for Windows provides automated analysis of network-based Microsoft Windows™ computer systems to determine the status of security patches. SafePatch determines what patches need to be installed on a system or group of systems. SafePatch collects and packages the necessary patches and the script to install those patches for the selected remote systems. SafePatch for Windows also supports browsing the Microsoft™ patch database and the viewing of the bulletins associated with the patches.

SafePatch for Windows has been tested for use on Windows 2000™ systems.

The SafePatch for Windows user interface consists of six tabbed panels corresponding to the six major components provided. The tabbed panels provided are ***Jobs***, ***Targets***, ***Evaluations***, ***Patches***, ***Packaged Updates*** and ***Settings***. This section summarizes the roles of each component.

1.1 Jobs Panel

The ***Jobs*** tabbed panel schedules and monitors two types of jobs: target jobs and host jobs. Target jobs schedule the evaluation, downloading of patches and creation of packaged updates for the computers being managed. Host jobs download the latest Microsoft™ patch database file or patch evaluation tools.

1.2 Targets Panel

The ***Targets*** tabbed panel defines the target computers and groups of computers that are to be managed. The target job scheduler on the ***Jobs*** panel allows you to select one of the targets defined here to be scheduled for evaluation, downloading of patches and creation of packaged updates. This panel also provides the status on the current operations being performed for each target.

1.3 Evaluations Panel

The ***Evaluations*** tabbed panel displays the detailed results from the computer evaluations including the associated bulletins of patches that need to be installed. Also displayed is the computer that is currently being evaluated. From this panel you can select the patch evaluation tool to be used for the evaluations.

1.4 Patches Panel

The ***Patches*** tabbed panel allows you to browse the Microsoft™ patch database to research information about the available patches. The ***Patches*** panel also reports the results of the patch downloads from Microsoft™ and what patches are currently being downloaded.

1.5 Packaged Updates Panel

The ***Packaged Updates*** panel allows you to view the update packages generated, organized by computer. An update package is a zip file containing the patches and an installation batch file needed to bring a target computer up to the latest patch level. When an individual update package is selected, the contents of the package can be browsed. From the package contents display, the ReadMe and installation batch file can be selected for display.

1.6 Settings Panel

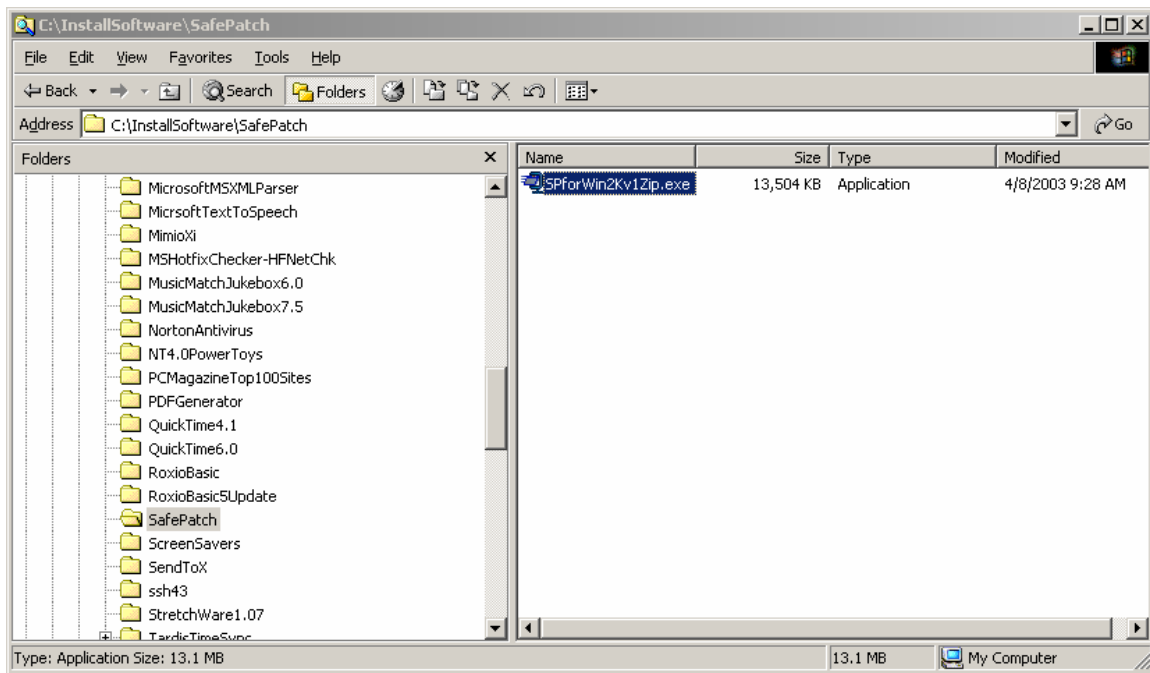
The ***Settings*** tabbed panel displays configuration and setting information for SafePatch for Windows. Some of the settings can be edited using this panel.

2. Getting Started

This chapter provides the basic steps required to start evaluating and creating patch packages for Windows™ computers.

2.1 Installing SafePatch for Windows

1. Execute the self-extracting zip file, SPForWin2KZip.exe, included in the distribution. You do this by double clicking on the zip file from the Windows™ file explorer. Choose the default location suggested by the extraction utility.



2. Run the j2re-1_4_02-windows-i586.exe program to install the Java Runtime Environment™, if you do not already have Java™ installed.
 - a. The j2re-1_4_02-windows-i586.exe program has been unzipped to the JavaJRE subdirectory.
 - b. To check if you already have the correct version of Java™ installed do the following.
 - i. Start a command prompt window. The command prompt window can usually be found by selecting the Windows™ **Start** button, followed by **Programs**, followed by **Accessories**, and finally **Command Prompt**.
 - ii. In the command prompt window type: **java -version**. If Java™ is installed, the computer response should be as follows:

```
java version "1.4.1_02"  
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.1_02-b06)  
Java HotSpot(TM) Client VM (build 1.4.1_02-b06, mixed mode)
```

3. You now need to install some supporting utilities used by SafePatch. SafePatch takes advantage of a few command utilities to provide key functionality. These utilities are incorporated in SafePatch to make their use almost transparent. Although all of these tools are freely available in the public domain, rules governing their redistribution vary. You must obtain some of these utilities directly

from the source and place them in the *C:\SafePatch\supportUtils* directory. In particular you will need to install one or more of the evaluation tools you want SafePatch to use. The supported evaluation tools are *HFNetChck* and *Mbascli*. Please see *Appendix E Support Utilities* for detailed information about the support utilities used by SafePatch for Windows. Included in the *c:\SafePatch\doc\user* directory of the distribution is an html file, *SupportUtilsReadme.html*, which includes information about the support utilities, including installation instructions, and links to the sites for obtaining them.

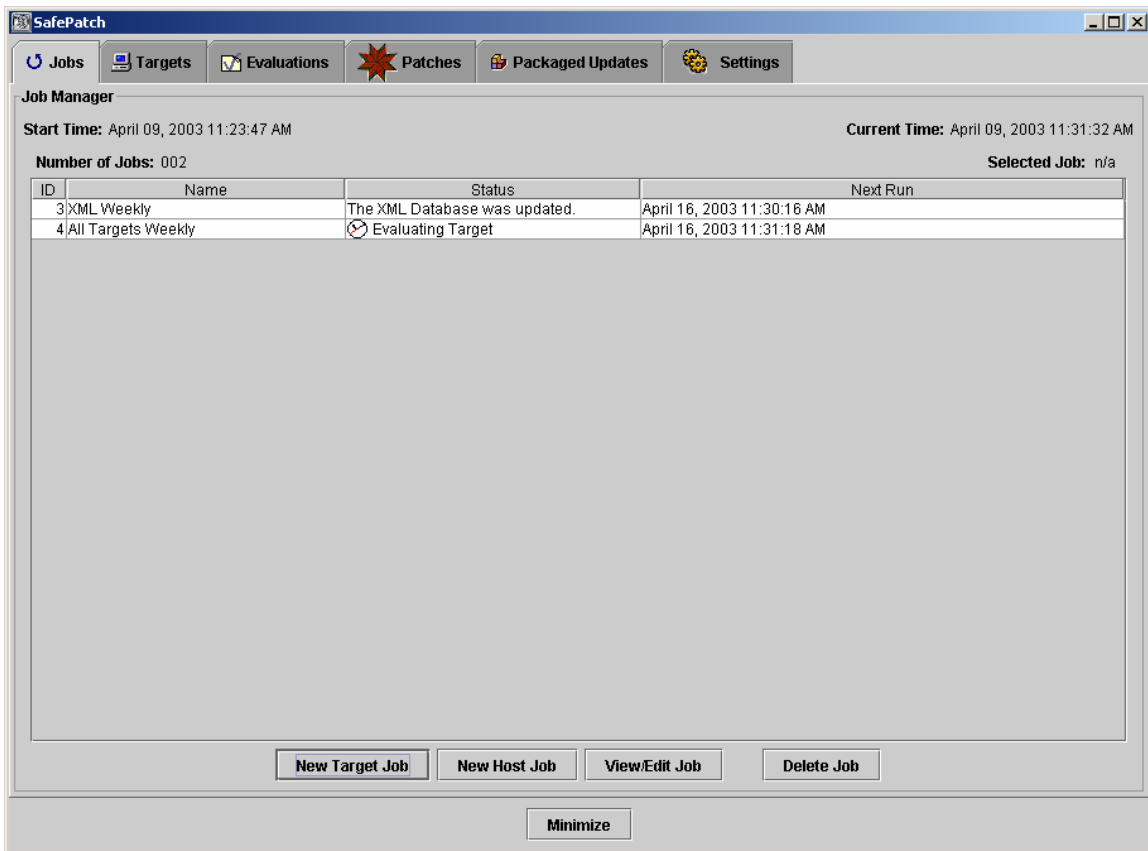
You have now successfully installed SafePatch for Windows and are ready to run it.

2.3 Starting SafePatch for Windows

To run SafePatch execute the *SafePatch.bat* file from the Windows™ file explorer or from a command prompt window. After SafePatch has finished its initializations, the following window will appear.



To display the main SafePatch display, click the left mouse button on the picture of the safe. You can return to the previous display at any time by left clicking on the **Minimize** button on the bottom of the SafePatch window. The main SafePatch display provides six tabbed panels: **Jobs**, **Targets**, **Evaluations**, **Patches**, **Packaged Updates** and **Settings**.



2.4 Creating A Host Job to Get the Latest Evaluation Database

You are now ready to create a host job to periodically update the evaluation database from Microsoft™.

1. From the **Jobs** tabbed panel select the **New Host Job** button located at the bottom of the panel.

Create Host Job

Host Job

Attributes

Job Name: Evaluation Database Update

Operations

☒ Update Evaluation Database

☐ Update Evaluation Tool

☐ Update Local Patch Database

Schedule

Begin

☒ As Soon As Possible

☐ At Specified Time

Initial Time

Date: April 01 2003

Time: 03:55 PM

Frequency

☐ Once

☒ Repeat

Interval

7 Days

0 Hours

0 Minutes

0 Seconds

0 Milliseconds

Apply Cancel

Create Cancel

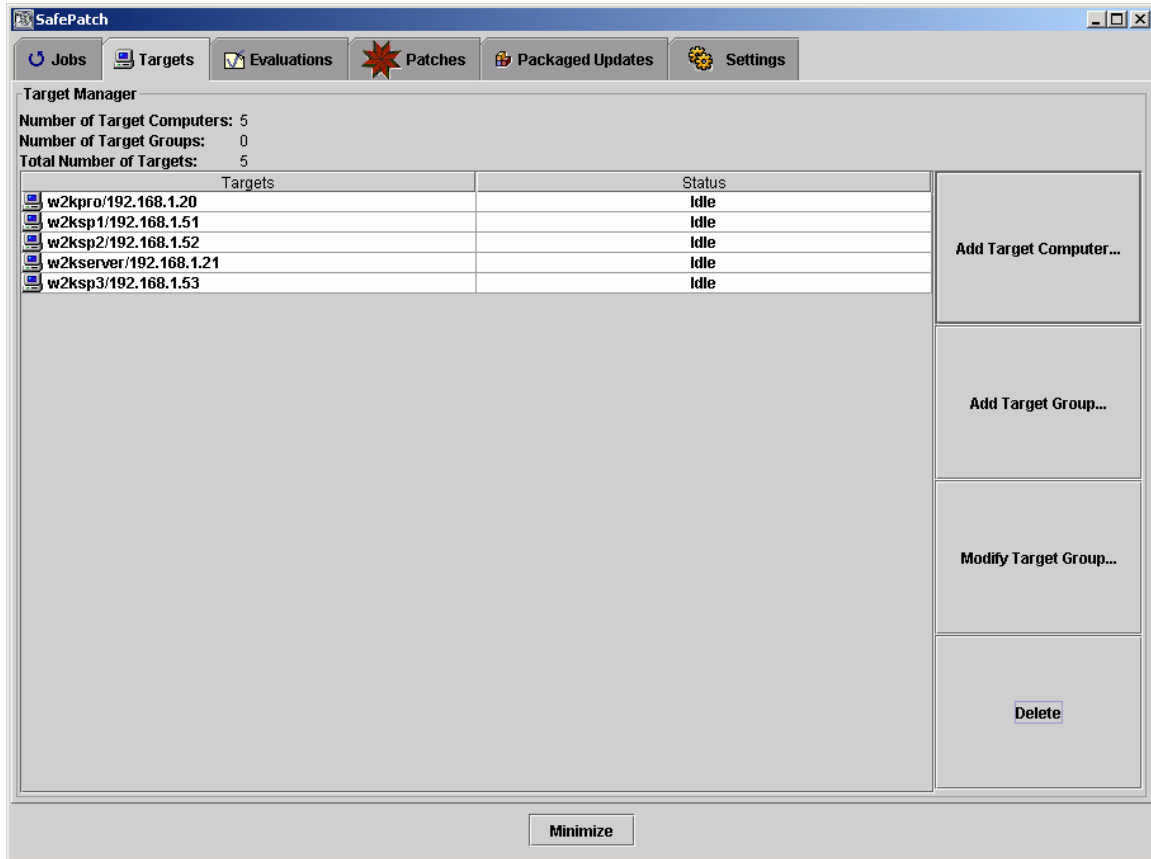
2. Type in a name for the job in the **Job Name** field in the upper left corner of the **Host Job** panel.
3. Select the **Update Evaluation Database** radio button in the **Operations** section.
4. In the **Schedule** section select the **As Soon As Possible** radio button in the **Begin** box, so that a new evaluation database will be retrieved as soon as the host job is created.
5. In the **Frequency** box, select the **Repeat** radio button and type in 7 in the **Days** field to have this job repeat once every week.
6. Press the **Apply** button in the **Schedule** section.
7. Press the **Create** button on the bottom of the **Host Job** panel.

This completes the creation of the host job. You should see the host job executing on the **Jobs** tabbed panel, which will download a new evaluation database file if a more current one is available.

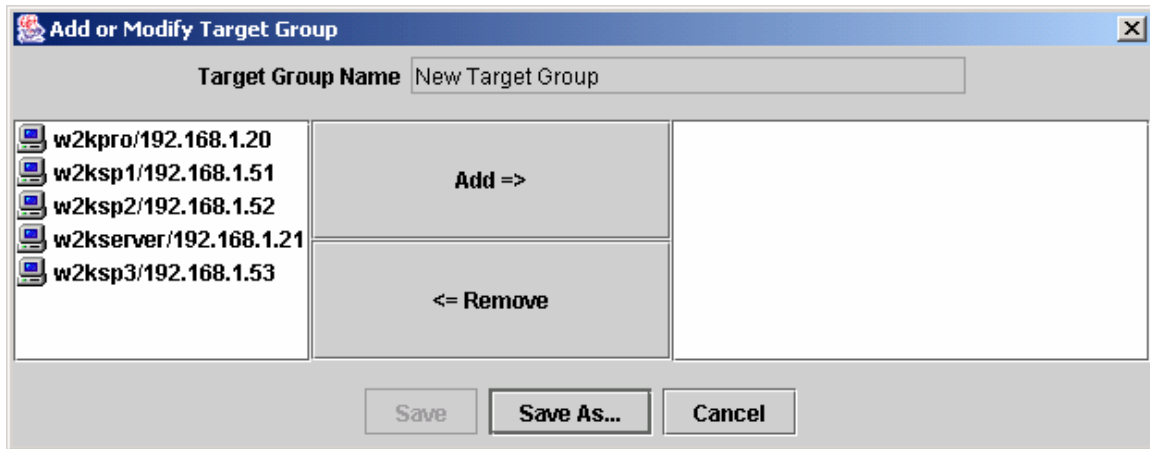
2.5 Adding Targets

The next step is to define a list of targets, either individual computers or groups of computers to evaluate and update.

1. Select the *Targets* tabbed panel.



2. Press the *Add Target Computer Button...* to start adding computers that you want to evaluate and update.
3. Type in the name of a computer in the *Add Target Computer* dialog box.
4. Select the **OK** button and the computer will be added to the list of targets.
5. Repeat steps 2 through 4 for each computer you want to evaluate and update.
6. Press the *Add Target Group Button...* to create a group of computers to schedule as a unit.



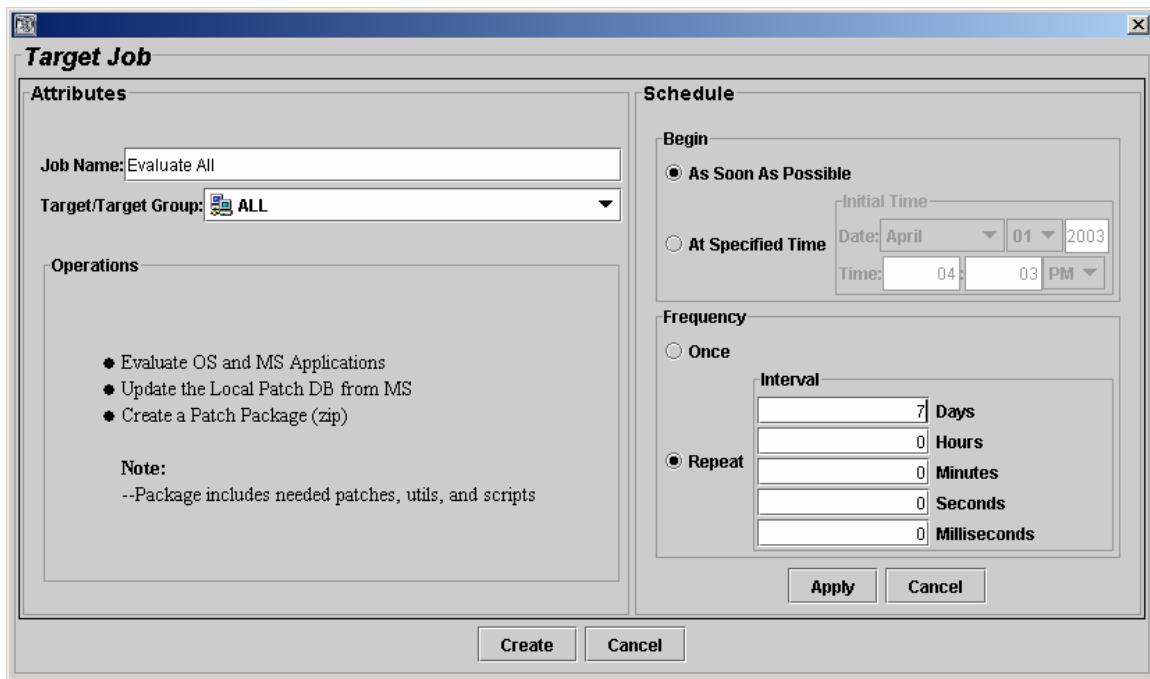
7. Select all of the target computers from the list of available computers on the left side and add them to the list of selected computers on the right side by pressing the **Add =>** button in the middle.
8. Press the **Save As...** button on the bottom of the dialog box.
9. Type in the name **ALL** to create a target group named **ALL**.
10. Press the **OK** button to complete the group creation.

You have now created a list of targets which includes individual computers and a group named **ALL** which contains all of the computers that you defined.

2.6 Creating a Target Job

The final step in setting up SafePath to evaluate your Windows™ computers is to create a target job.

1. From the **Jobs** tabbed panel select the **New Target Job** button located at the bottom of the panel.

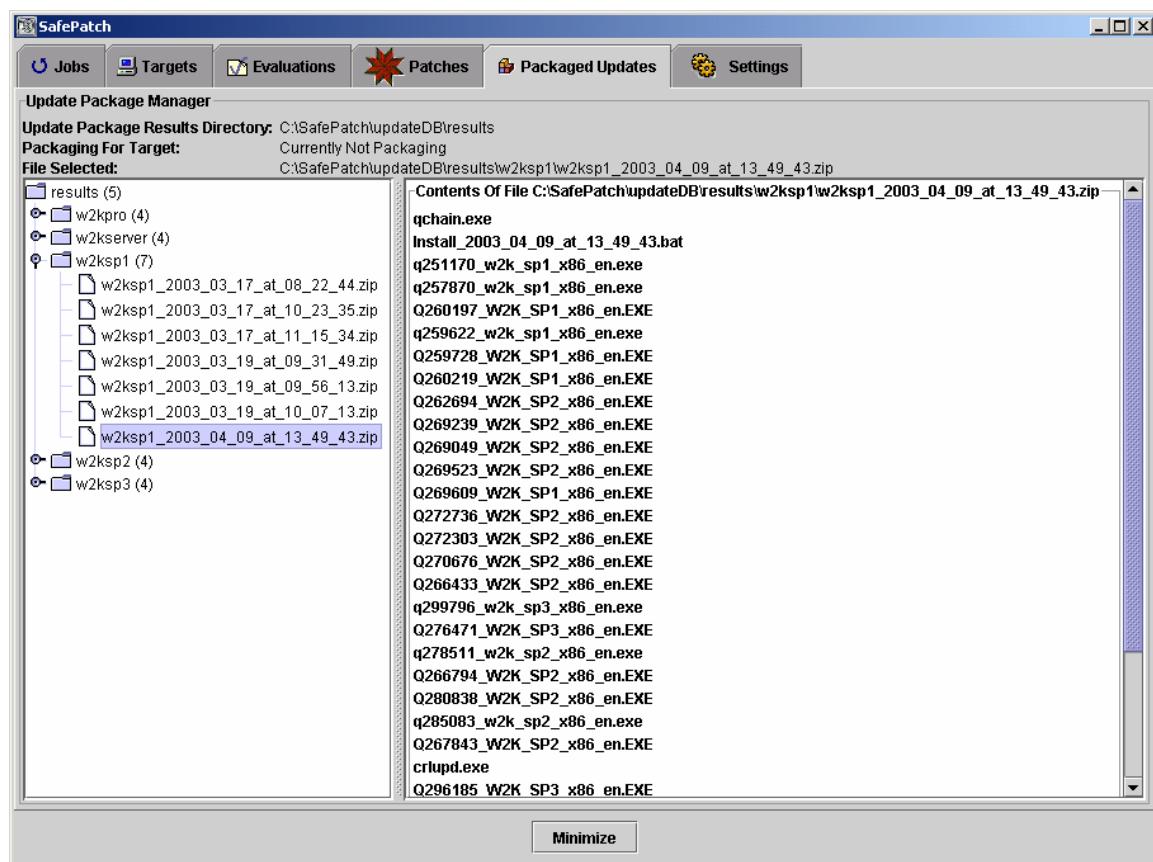


2. Type in a name for the job in the **Job Name** field in the upper left corner of the **Target Job** panel.

3. Select the target group **ALL** from the **Target/Target Group** drop down list.
4. In the **Schedule** section select the **As Soon As Possible** radio button in the **Begin** box, so that the first evaluation and installation package will be created as soon as the target job is created.
5. In the **Frequency** box, select the **Repeat** radio button and type in 7 in the **Days** field to have this job repeat once every week.
6. Press the **Apply** button in the **Schedule** section.
7. Press the **Create** button on the bottom of the **Target Job** panel.

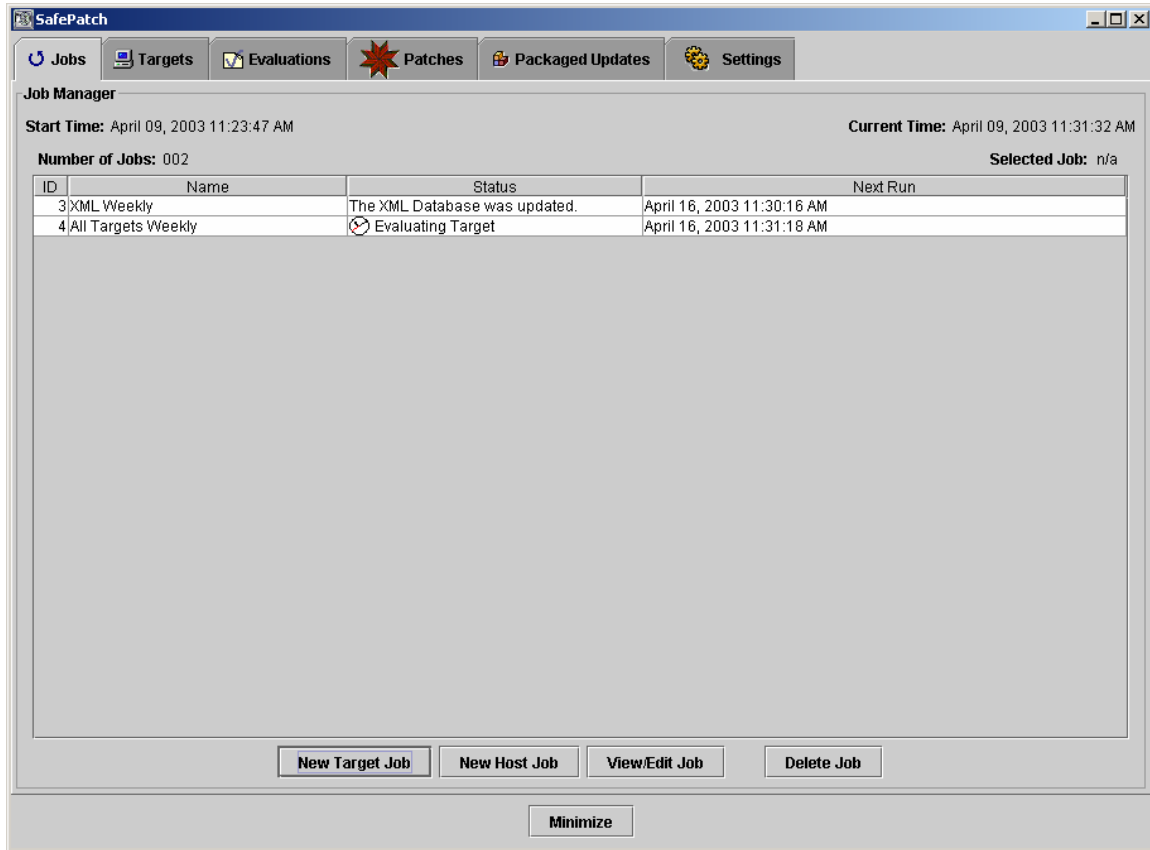
This completes the creation of the target job. You should see the target job executing on the **Jobs** tabbed panel and see running indications in the other tabbed panels as it progresses through the job. After the target job completes you can view the results from each of the steps in the various tabbed panels.

2.7 Viewing the Packaged Updates (Installation Packages)



After the target job created in the previous section completes, a zip file will be created for each of the target computers in the **ALL** target group. You can browse the zip files created using the **Packaged Updates** tabbed panel. The directory containing the latest zip file created for each of the computers evaluated is displayed in the **Update Package Results Directory** field. The zip files are named <target computer name>.zip, where <target computer name> is the name that you entered when creating the target computer. Also contained in the update package results directory are subdirectories corresponding to the target computers. These target computer subdirectories contain copies of all of the zip files created for each of the computers. Please see section 9 *Interpreting The SafePatch Evaluation Results* for the recommended use of the target job results.

3 Jobs Panel



The **Jobs** panel schedules and monitors two types of jobs: target jobs and host jobs. Target jobs schedule the evaluation, downloading of patches and creation of packaged updates for the target computers being managed. Host jobs download the latest Microsoft™ patch database file or patch evaluation tools used by the host computer (the computer on which SafePatch is being run).

The **Start Time** field in the top left-hand corner indicates the time and date the SafePatch program was last started. The **Current Time** field in the top right-hand corner shows the current date and time being used by your computer.

The next two fields from the top **Number of Jobs** and **Selected Job** indicate the total number of jobs and the currently selected job respectively. You can select a job by clicking on it in the table below these fields. The selected job can then be viewed in detail by clicking on the **View/Edit Job** button located below the table or it can be deleted by clicking on the **Delete Job** button.

The table in the middle of the panel displays the jobs that have been scheduled including its job identifier, the user specified name, the status of the job and the next run time. The next run time is the next time the job is scheduled to run. For onetime jobs that have already completed (i.e., the job will no longer be run), the next run time displays the time the job ran.

The **New Target Job** button and the **New Host Job** button start the **Target Job** and **Host Job** panels respectively. The **Target Job** and **Host Job** panels are used for creating new jobs.

3.1 Target Job Panel

The screenshot shows the 'Target Job' dialog box with the following details:

- Attributes:**
 - Job Name: Evaluate All
 - Target/Target Group: ALL
- Operations:**
 - Evaluate OS and MS Applications
 - Update the Local Patch DB from MS
 - Create a Patch Package (zip)
 - Note:**
--Package includes needed patches, utils, and scripts
- Schedule:**
 - Begin:**
 - ☒ As Soon As Possible
 - ☐ At Specified Time (Initial Time: Date: April 01 2003, Time: 04:03 PM)
 - Frequency:**
 - ☐ Once
 - ☒ Repeat (Interval: 7 Days, 0 Hours, 0 Minutes, 0 Seconds, 0 Milliseconds)

Buttons at the bottom: Create, Cancel, Apply, Cancel.

The **Target Job** panel is used for creating new target jobs. It is started from the **Jobs** tabbed panel by pressing the **New Target Job** button. The **Job Name** field provides a place for you to type in a descriptive name for the target job. This is the name that is displayed on the main **Jobs** panel for the job or when you choose to view the job.

The **Target/Target Group** drop-down selection list allows you to select a target computer or group to associate with this target job. You simply click on the selection list field and the available targets will be displayed. Select the desired target by moving to it with the cursor, which will highlight it.

The **Operations** section specifies the operations that will be executed by the target job. The target job will be evaluated for operating system and Microsoft™ application patches, the required patches will be downloaded and a patch package (update package zip file) will be created for the computers.

The **Schedule** section of the **Target Job** panel allows you to specify when and how often the target job runs. First you select when the job should initially start by filling in the **Begin** section. You can either select the **As Soon As Possible** radio button to start the job as soon as it is created or the **At Specified Time** radio button to specify the starting date and time using the **Initial Time** fields. The next step is to specify how often the job should be run by filling in the **Frequency** section. Select either the **Once** radio button to have the job run only one time or the **Repeat** radio button to have it run periodically at the interval specified by the **Interval** fields. After the Schedule has been selected, press the **Apply** button to use the schedule specified. When filling in values for the schedule, you can press the **Cancel** button to revert back to the last schedule applied.

When you are finished, press the **Create** button on the bottom of the **Target Job** panel to create the job. To close the panel without creating a new job, press the **Cancel** button.

3.2 Host Job Panel

Create Host Job

Host Job

Attributes

Job Name: Evaluation Database Update

Operations

- ☒ Update Evaluation Database
- ☐ Update Evaluation Tool
- ☐ Update Local Patch Database

Schedule

Begin

- ☒ As Soon As Possible
- ☐ At Specified Time

Initial Time

Date: April 01 2003

Time: 03:55 PM

Frequency

- ☐ Once
- ☒ Repeat

Interval

7 Days

0 Hours

0 Minutes

0 Seconds

0 Milliseconds

Apply Cancel

Create Cancel

The **Host Job** panel is used for creating new host jobs. It is started from the **Jobs** tabbed panel by pressing the **New Host Job** button. Host jobs download the latest Microsoft™ patch database file or patch evaluation tools used by the host computer (the computer on which SafePatch is being run). The **Job Name** field provides a place for you to type in a descriptive name for the target job. This is the name that is displayed on the main **Jobs** panel for the job and when you choose to view the job.

The **Operations** radio button section allows you to select whether this host job updates the patch database file, the evaluation tool from Microsoft™, or updates the database of patches downloaded from Microsoft™. The **Update Local Patch Database** option downloads patches based on all the evaluation files generated and stored in the evaluation directory. This feature is useful for gathering patches for systems that are not connected to the internet (e.g. a classified network).

To gather patches for such systems, copy the evaluation files from the isolated network or computer and place them on a computer connected to the internet. On the **Settings** tabbed panel, change the evaluation directory to point to the directory where you copied the evaluation files. Next, run an **Update Local Patch Database** host job to collect the necessary patches. Then copy the patches to the isolated network or computer and run a target job to evaluate and create the update packages (patch zip files) for the isolated computers.

The **Schedule** section of the **Host Job** panel allows you to specify when and how often the host job runs. First, select when the job should initially start by filling in the **Begin** section. You can either select the **As Soon As Possible** radio button to start the job as soon as it is created or the **At Specified Time** radio button to specify the starting date and time using the **Initial Time** fields. The next step is to specify how often the job should be run by filling in the **Frequency** section. Select either the **Once** radio button to have the job run only one time or the **Repeat** radio button to have it run periodically at the interval specified by the **Interval** fields. After the schedule has been selected, press the **Apply** button to use the

schedule specified. When filling in values for the schedule, you can press the **Cancel** button to revert back to the last schedule applied.

When you are finished, press the **Create** button on the bottom of the **Host Job** panel to create the job. To close the panel without creating a new job, press the **Cancel** button.

3.3 Job Properties Panel

Target Job Properties

Job Properties

Job ID: 002

Job Name: All Targets Weekly

Job Type: Create Package of Patches for Target

Target Name: ALL TARGETS

IP Address: N/A

Status:

Current: Creating Target Installation Package for w2ksp2/192.168.1.52 (3 of 5)

Run #	Status
0	Idle
1	Starting to create the Target installation package
1	Creating Target Installation Package for w2kpro/192.168.1.20 (1 of 5)
1	Creating Target Installation Package for w2ksp1/192.168.1.51 (2 of 5)
1	Creating Target Installation Package for w2ksp2/192.168.1.52 (3 of 5)

Listeners: 003

Schedule

Begin

☐ As Soon As Possible

☒ At Specified Time

Initial Time

Date: April 10 2003

Time: 04:12 PM

Frequency

☐ Once

☒ Repeat

Interval

7 Days

0 Hours

0 Minutes

0 Seconds

0 Milliseconds

Apply Cancel

Times Run: 001

Last Run: April 10, 2003 04:12:47 PM

Next Run: April 17, 2003 04:12:47 PM

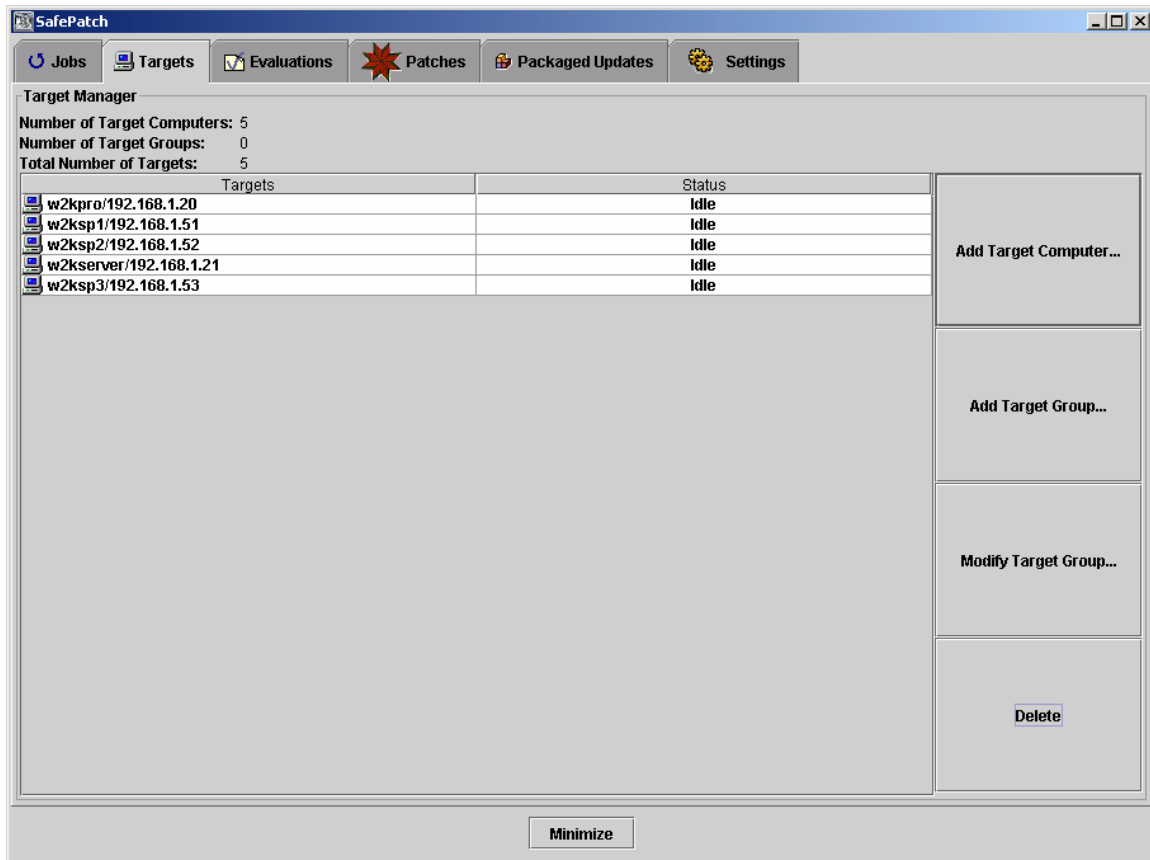
Apply Cancel OK

The **Job Properties** panel displays detailed information about the job. It is started from the **Jobs** tabbed panel by selecting a job from the table and pressing the **View/Edit Job** button. The **Job Properties** panel displays detailed information about the selected job. The upper left-hand corner displays the user specified job name, the type of job, the computer or computer group associated with the job and the IP address of the computer associated with the job. The status section in the lower left-hand corner displays a history of the job. The right-hand side of the **Job Properties** panel displays the scheduling information, number of times it has run and the last and next time the job is scheduled to run.

3.4 Delete Job

The **Delete Job** button on the bottom of the **Jobs** tabbed panel deletes any selected jobs in the job table. It will also delete any onetime jobs from the job table that have been completed, since they no longer will be scheduled to run.

4 Targets Panel

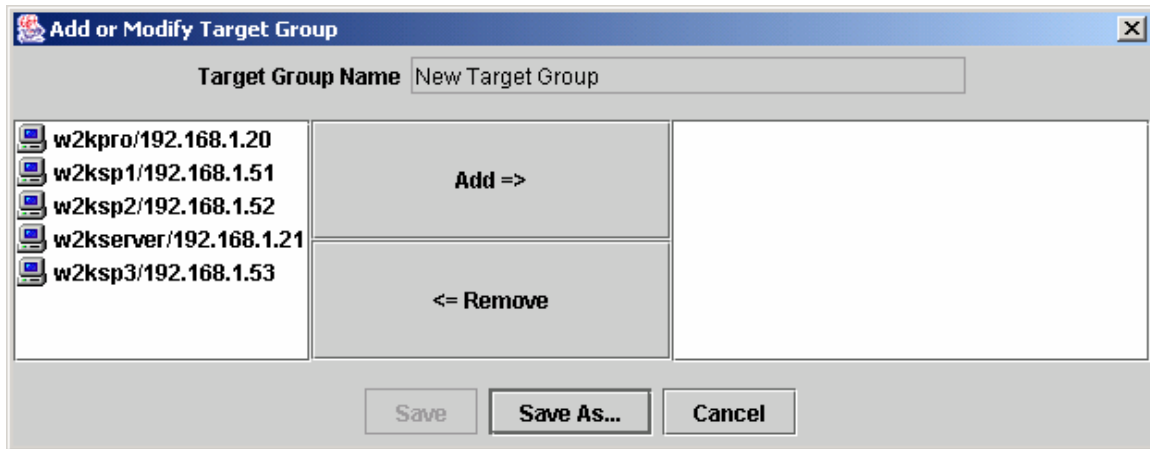


The **Targets** tabbed panel is used for managing the targets, either individual target computers or target groups. The target computers are computers that you have administrator rights on that you want to evaluate, download patches, and create packaged updates (see Appendix B *Administrator Privileges* for details on how to establish administrator rights). A target group is a collection of target computers that can be scheduled in a job as a unit.

The top portion of the **Targets** tabbed panel contains statistics on the number and types of targets available. The middle portion contains a table of the names and IP addresses of the targets and their current operating status. Target computer names are displayed in lowercase, have an icon with a single computer, and display the IP address. Target group names are displayed in uppercase and have an icon with two computers. Targets can only be associated with one job. If a target is associated with a job, its name will be displayed dimmed.

The buttons to the right of the table allow you to manage the targets. The **Add Target Computer...** button starts the **Add Target Computer** dialog box requesting the name of a computer you want to add to the list. Type in the name of a computer and select the **OK** button and the computer will be added to the list of targets.

The **Add Target Group...** button starts the **Add or Modify Target Group** dialog box.

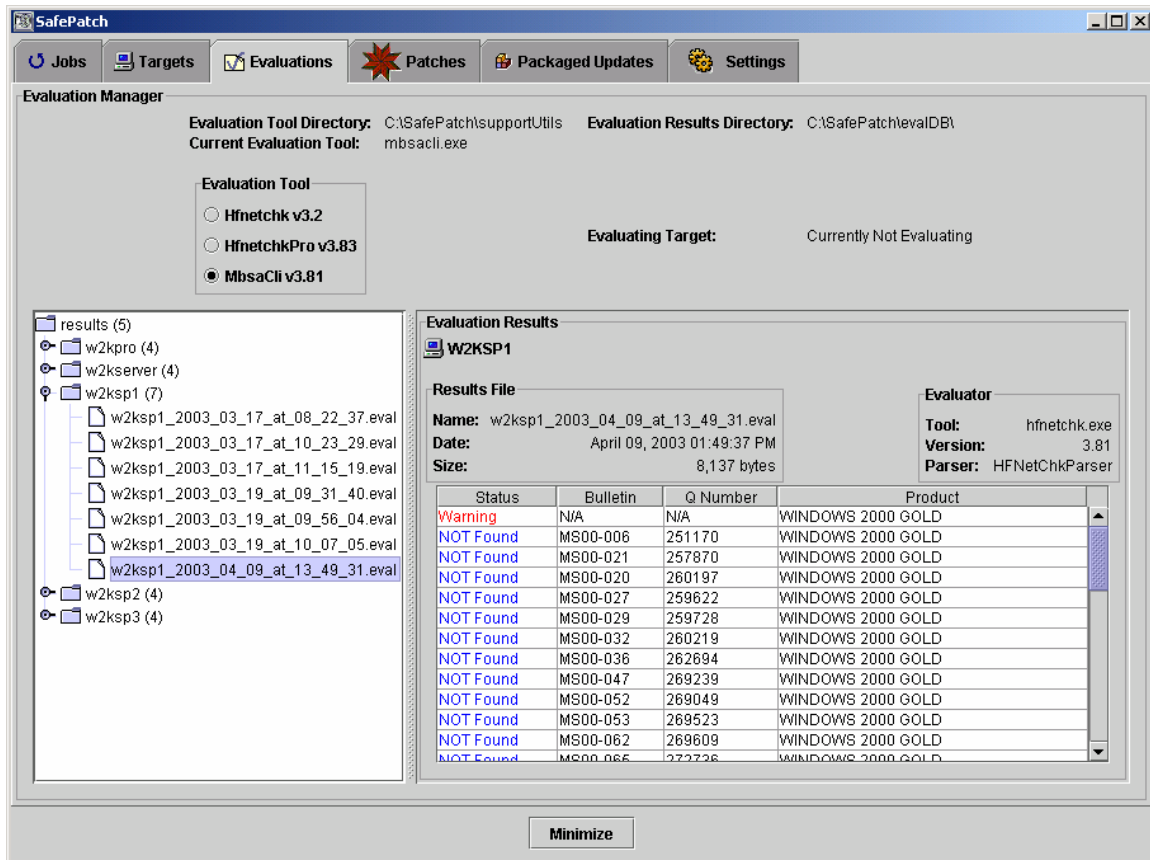


The **Add or Modify Target Group** dialog box lists the computers in the target group in the right-hand panel and the list of available computers in the left-hand panel. Select computers in the left-hand panel and press the **Add =>** button to add computers to the group; select computers in the right-hand panel and press the **<= Remove** button to remove computers from the group. A computer whose name is dimmed indicates the computer is currently associated with an existing job. Being associated with an existing job does not prevent it from being added or removed from the group. To save the group, press the **Save As...** button and you will be prompted for a name. Type in a name for the group and press the **OK** button to create the group. To exit the **Add or Modify Target Group** dialog box without creating a target group press the **Cancel** button.

Selecting one or more target groups and pressing the **Modify Target Group...** button also starts the **Add or Modify Target Group** dialog box displaying the current members of the selected target group. The **Save** button is available in addition to the **Save As...** button, enabling you to save the group with the same name after modifying it.

To delete targets from the list of available targets, select them from the target table in the middle of the **Targets** tabbed panel and press the **Delete** button on the lower right portion of the panel. Targets that are associated with a job are displayed dimmed and cannot be deleted. The jobs associated with these targets must be deleted first before the target can be deleted. If you try and delete a target computer that is part of a target group, you will be warned that it is part of a group and it will automatically be removed from the group if you confirm the deletion.

5 Evaluations Panel



The **Evaluations** tabbed panel provides information about the evaluation of the target computers. The top portion of the panel contains the following fields.

Evaluation Tool Directory	The directory containing the tools used for evaluating the target computers. The currently supported tools are Hfnetchk, HfnetchkPro, and MbsaCli. The tools you wish to use with SafePatch should be installed in this directory.
Evaluation Results Directory	The directory where the evaluation reports and the Microsoft™ patch databases are stored.
Current Evaluation Tool	The name of the evaluation tool currently being used by SafePatch.
Evaluation Tool	The radio box selection for choosing which evaluation tool should be used by SafePatch.
Evaluating Target	The target computer currently being evaluated.

The split pane on the **Evaluations** tabbed panel displays a results tree organized by target computer name on the left side. As you navigate the results tree, information about the directory or an **Evaluations Results** panel is displayed on the pane on the right corresponding to the selected node in the tree. The directory names correspond to the computer names whose evaluation results the directory contains. The number in parenthesis next to the computer name indicates how many evaluation results files are in the directory.

The **Evaluations Results** panel displays information about a results file. The top portion of the panel displays information about the target computer being evaluated, the name and statistics for the results file,

and the evaluation tool used to generate the evaluation results file. The table on the bottom of the panel displays information from the content of the results file. It displays the reported status, the applicable bulletin number, the Microsoft™ assigned Q Number and the affected product. Clicking on a row in the table brings up a detailed summary of the information from the selected entry in the results file. See section 9 *Interpreting The SafePatch Evaluation Results* for detailed information on interpreting and using the evaluation results.

MS02-042:

Evaluation Results

Bulletin:
MS02-042

Q Number:
326886

Product:
WINDOWS 2000 SP2

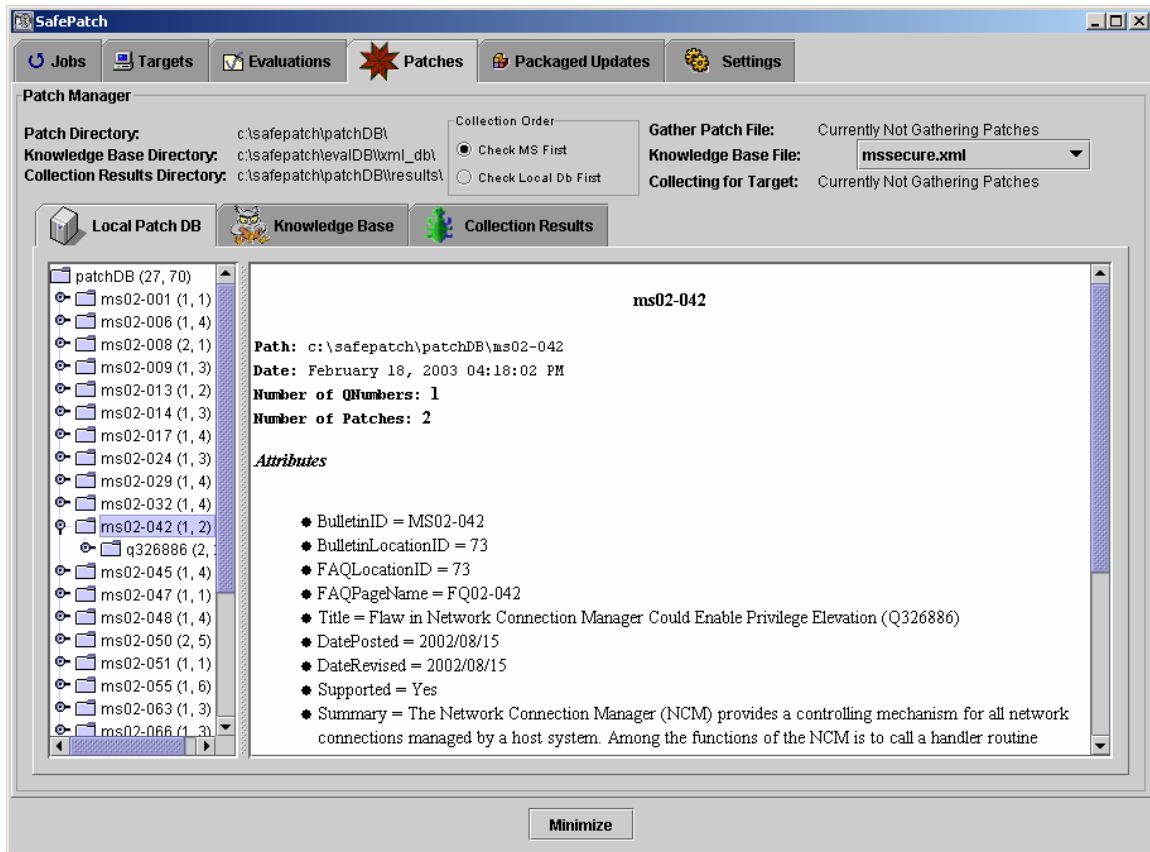
Machine Name:
W2KSP2 (192.168.1.52)

IP:
192.168.1.52

Status:
NOT Found

Reason:
File \\w2ksp2\C\$\WINNT\system32\netman.dll has a file version [5.0.2195.2779] that is less than what is expected [5.0.2195.5974].

6 Patches Panel



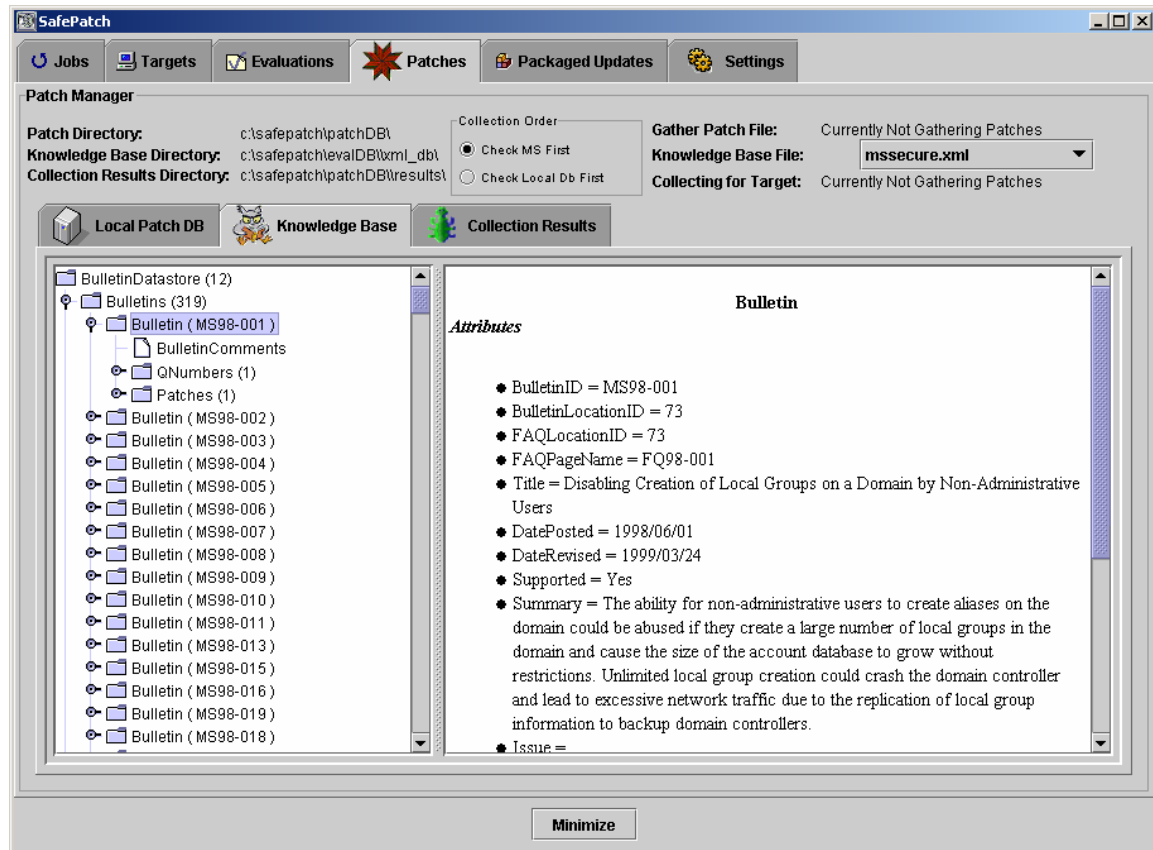
The **Patches** tabbed panel displays information about patches and the Microsoft™ patch database file, mssecure.xml. The top portion of the panel displays the following information.

Patch Directory	The directory where the collected patches are stored.
Knowledge Base Directory	The directory where the Microsoft™ patch database files (mssecure.xml) are stored.
Collection Results Directory	The directory containing the log files for the patch collecting (i.e. downloading/gathering).
Collection Order	Radio button specifying whether to check the Microsoft™ website or the local database (Local Patch DB) first when collecting patches. You would check the local database first if you were interested in getting the fastest retrievals. You would check Microsoft™ first if you suspect that Microsoft™ may have updated patches without changing the <i>ms</i> and <i>q</i> numbers for the patch and always wanted to check the Microsoft™ site for the latest patch.
Gather Patch File	The name of the current patch being collected.
Knowledge Base File	Selection of the version of the Microsoft™ patch database to be used for evaluating of computers and collecting of patches.
Collecting for Target	The target computer whose patches are currently being collected.

6.1 Local Patch DB

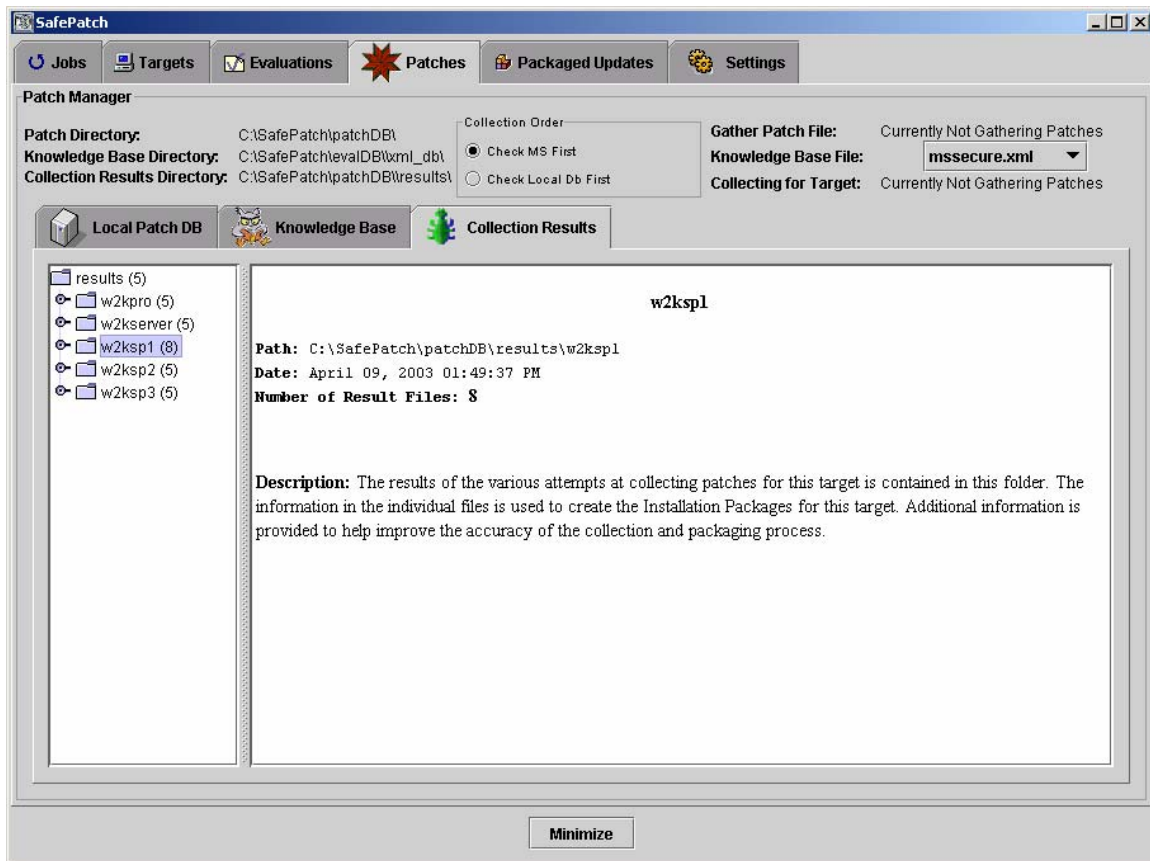
The **Local Patch DB** panel is a split pane panel that allows you to browse the local database of patches collected (i.e. downloaded/gathered). The left pane displays the patch tree organized by bulletin identifier. The number pair in parenthesis on a node represents the number of child nodes and the number of patches contained within the node. Clicking on a bulletin identifier node (msxx-xxx) displays information from the bulletin in the right pane. Clicking on a node corresponding to a patch displays detailed information about the patch.

6.2 Knowledge Base



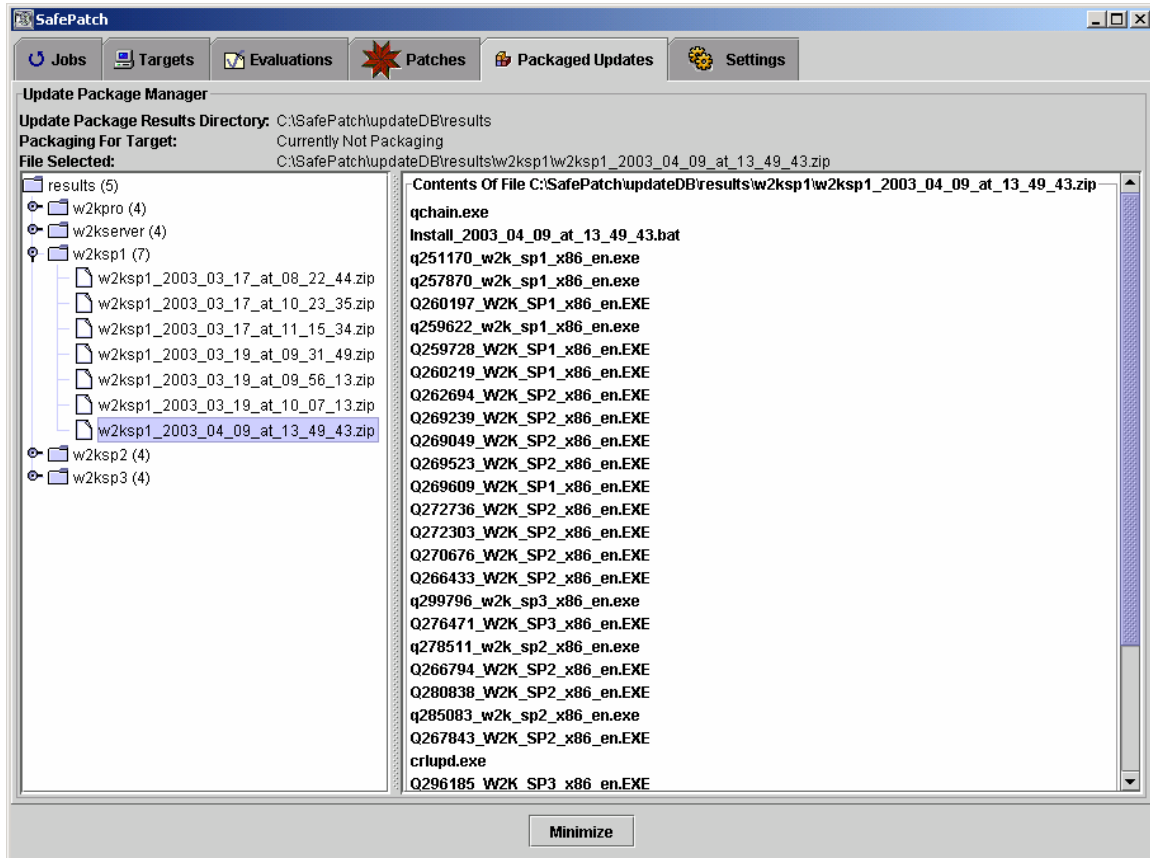
The **Knowledge Base** panel allows you to browse the information contained in the Microsoft™ patch database file (mssecure.xml). The panel consists of a split pane panel with a tree display of the nodes in the database file in the left pane and information about the selected node in the right pane. Double clicking on some of the field names in the right pane will bring up more detailed information about the selected field.

6.3 Collection Results



The **Collection Results** panel allows you to view the collection results files, which displays a history of the collections performed organized by the target computers for which they were collected. The panel consists of a split pane which displays a results tree in the left pane and information about the selected node in the right pane. The computer nodes in the results tree display the number of collection results files for that computer in parenthesis after the name of the computer. The right pane displays either information about the target computer directory or the contents of the collection results file depending on what kind of node is selected in the results tree.

7 Packaged Updates Panel



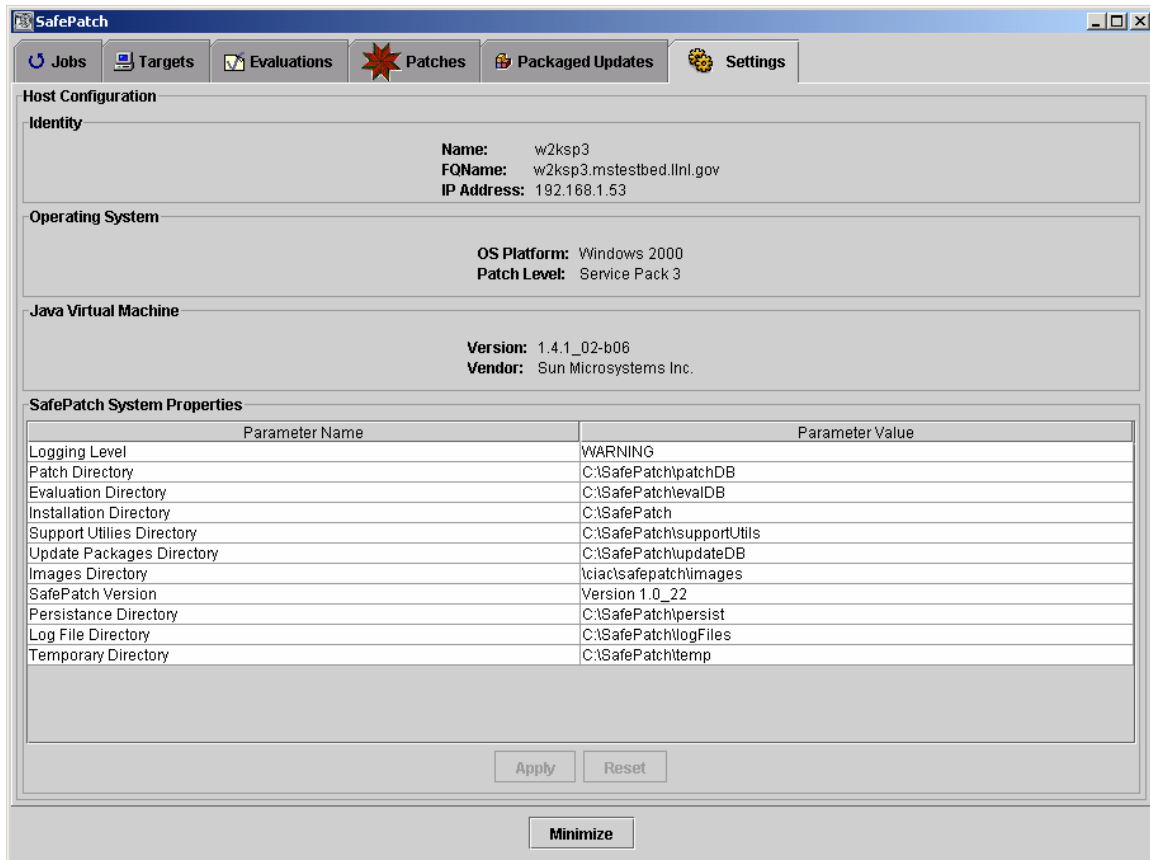
The **Packaged Updates** tabbed panel displays information about the packaged updates (installation zip files). The top portion of the panel displays the following information.

Update Package Results Directory	<p>The directory containing the latest packaged updates (installation zip files) created for each of the computers evaluated. The zip files are named <target computer name>.zip, where <target computer name> is the name that you typed when creating the target computer.</p> <p>Also contained in the <i>Update Package Results Directory</i> are subdirectories corresponding to the target computers. These target computer subdirectories contain dated copies of all of the zip files created for each of the computers.</p>
Packaging For Target	The target computer for which an update package is currently being created.
File Selected	The name and directory location of the file selected in the update package tree in the split pane panel.

The bottom section of the **Packaged Updates** tabbed panel displays a split pane panel, which allows you to browse the available update packages. The left pane contains the update package tree organized by target computer. Selecting a node displays either information about the directory selected or the update package selected depending on the type of node. When viewing an update package file, a listing of the contents of

the update package is displayed in the right pane. Clicking on the ReadMe<date>.html file, where <date> is the date it was created, causes the ReadMe file to be displayed in a separate panel. Clicking on Install<date>.bat will display the installation batch file in a separate panel.

8 Settings Panel



The **Settings** tabbed panel displays configuration and setting information for SafePatch for Windows. The top portion of the panel displays information about the computer on which SafePatch for Windows is running (i.e. the host computer). Information includes the host name and IP address, the operating system and version, and the java virtual machine being used.

The bottom portion of the panel displays the SafePatch configuration parameters/properties table. Some of the parameters can be modified, others are for display only. The parameters and their definitions are as follows.

Parameter Name	Description	Modifiable
Logging Level	Controls the level of messages that are logged to the application log. The application log provides information for tracking the status history of SafePatch operations performed. The logging levels range from OFF (no logging) to ALL (log all messages).	yes
Patch Directory	The directory where patches are collected and saved.	yes
Evaluation Directory	The directory where the evaluation reports and the Microsoft™ patch databases are stored.	yes
Installation Directory	Root directory where SafePatch is installed. The only way this value can be changed is with the command line option <code>-id</code> . See Appendix C SafePatch Command Line for more details.	no

Support Utilities Directory	Directory containing utility programs used by SafePatch (e.g. the evaluation engines). This is a fixed directory relative to the <i>Installation Directory</i> .	no
Update Package Directory	Directory containing the update packages that were created. This is a fixed directory relative to the <i>Installation Directory</i> .	no
Images Directory	The directory where the icons used by SafePatch are stored. This is a fixed directory relative to the <i>Installation Directory</i> .	no
SafePatch Version	The version of SafePatch for Windows that is running.	no
Persistence Directory	The directory where information stored between invocations of the SafePatch program is stored. This is a fixed directory relative to the <i>Installation Directory</i> .	no
Log File Directory	Directory where log files are stored. This is a fixed directory relative to the <i>Installation Directory</i> .	no
Temporary Directory	Directory where temporary files are stored. This is a fixed directory relative to the <i>Installation Directory</i> .	no

To change one of the parameters, left click on the Parameter Value and an editor for that value will be presented. After you have made your parameter changes, left click the ***Apply*** button on the bottom to apply the changes. Left click the ***Reset*** button to discard the current parameter changes.

9 Interpreting The SafePatch Evaluation Results

This section describes the evaluation results and how to interpret them. Items 1 – 3 contain recommended steps for using the results produced by running a *Target Job*.

- | |
|--|
| 1) Select the Evaluations tabbed panel and look at the most recently generated evaluation results generated for the machine of interest. Clicking on any row in the evaluation results will display more detailed information. |
| 2) Look for rows in the report with a status of Information and click on them. These rows will provide you with information about the evaluation. For example the error message “Error: Admin rights are required to scan” is displayed when you do not have administrator rights for the evaluated target computer and you click on the row. |
| 3) Look for rows in the report with a status of Warning and click on them. These rows typically contain information informing you to upgrade the target computer to the latest service packs. It is recommended that you install the specified service packs and then reevaluate the target computer by scheduling another target job once the service packs have been installed. Patch evaluation of the target computer is dependent on the service pack level that is installed. |
| 4) Rows with a status of NOT Found correspond to patches that will be downloaded and included in the target computer’s update package. |
| 5) Rows with a status of Note usually refer you to additional bulletin or knowledge base articles and do not contain information critical to the use of SafePatch. |

Appendix A Glossary

Evaluation Database	The Microsoft™ XML file that specifies the patches available and information about those patches.
Host	The computer on which SafePatch for Windows is being run.
Host Job	A job scheduled to either update the Microsoft™ database or download the latest version of the evaluation tool on the host.
Installation Zip File	See <i>update package</i> .
Job	A scheduled task, either a target job or a host job.
Local Patch DB	The local repository or database of patches collected from Microsoft™.
Packaged Update	See <i>update package</i> .
Target	Either a target computer or target group to be evaluated for needed patches and for which a patch installation package will be created.
Target Computer	A computer to be evaluated for needed patches and for which a patch installation package will be created.
Target Group	One or more target computers grouped together to form a single entity for scheduling target jobs.
Target Job	A job scheduled to evaluate, download patches, and generate an update package for a target computer or target group.
Update Package	A zip file consisting of the patches, an installation batch file, and a readme.html file. These are the necessary components for bringing your computer up to the latest patch level.

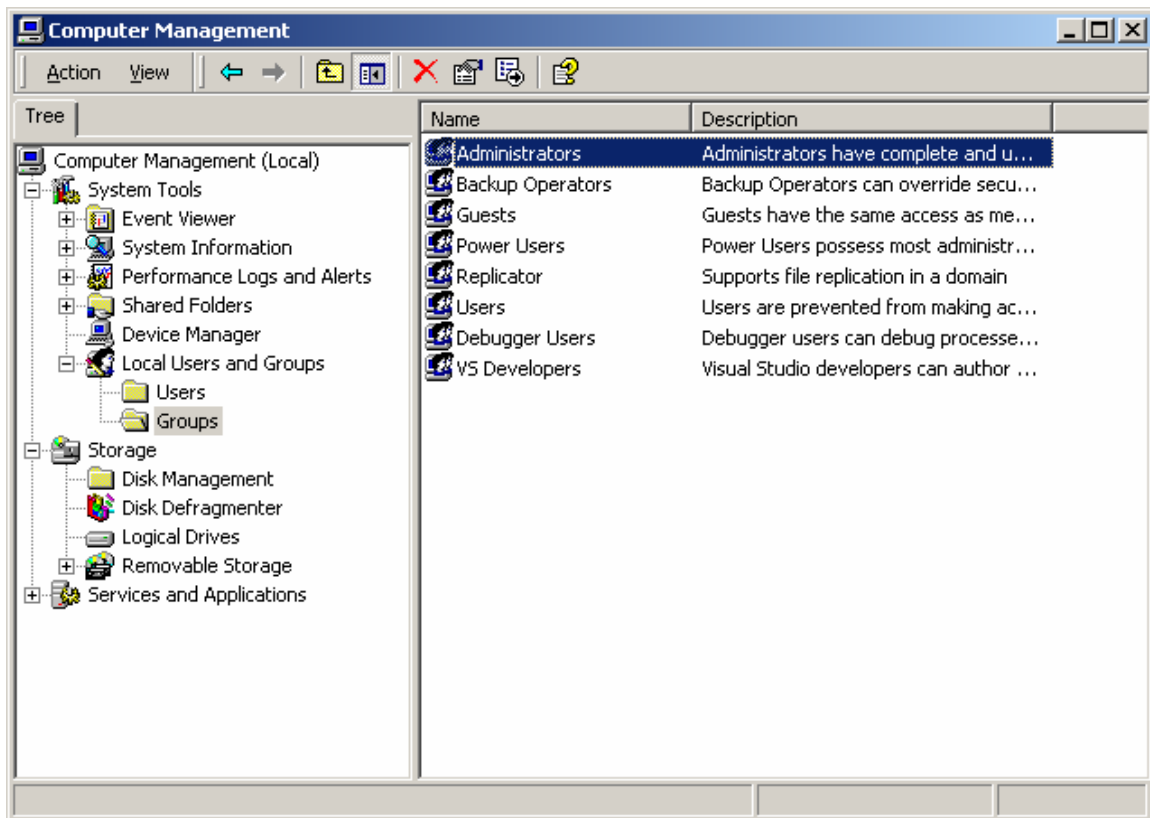
Appendix B Administrator Privileges

In order to use SafePatch for Windows, the user account under which you are running SafePatch for Windows must have administrator privileges. Administrator privileges are available by either being a member of the *Domain Admins* group or a member of the *Administrator* group on each of the local computers you want to manage using SafePatch.

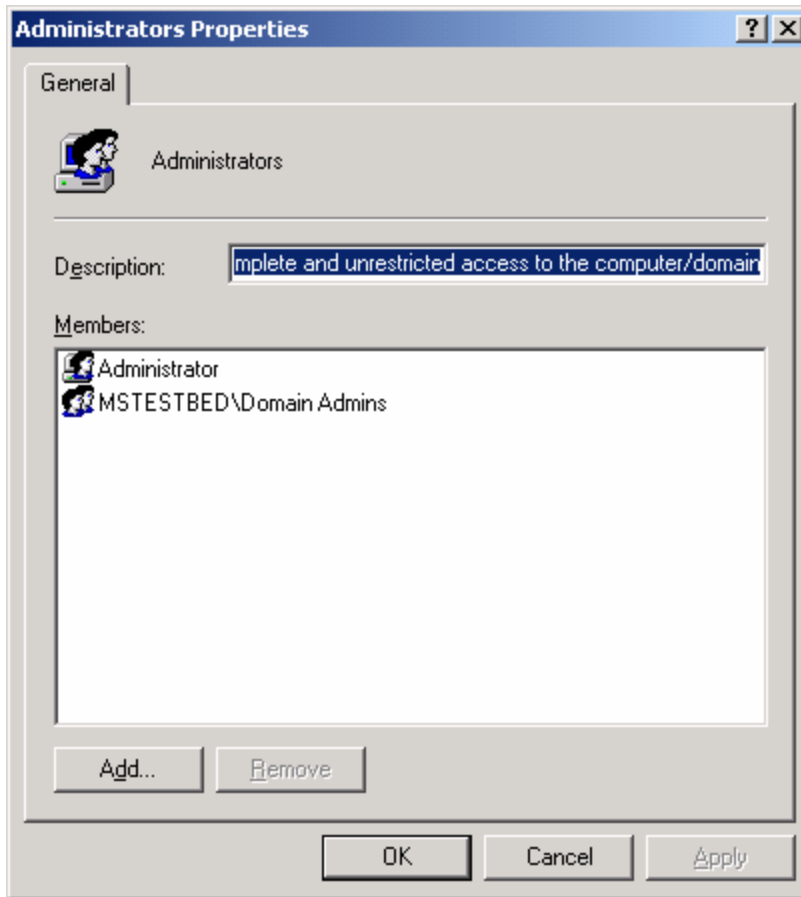
One way to give administrator privileges to people you expect to run SafePatch on your domain is to create a domain group on your server called *SafePatch Administrator*, or a similar name of your choice. Then, add the users you want to be able to run SafePatch to the *SafePatch Administrator* group. Once this group is created you can add this domain group to the local *Administrator* group on each of the computers you want to manage with SafePatch. In this manner any change to the users you want to be able to manage with SafePatch will automatically be reflected on each of the managed computers by simply changing the membership of the *SafePatch Administrator* group.

The steps required to add a user or user group to the *Administrator* group on a local Windows 2000 computer is as follows.

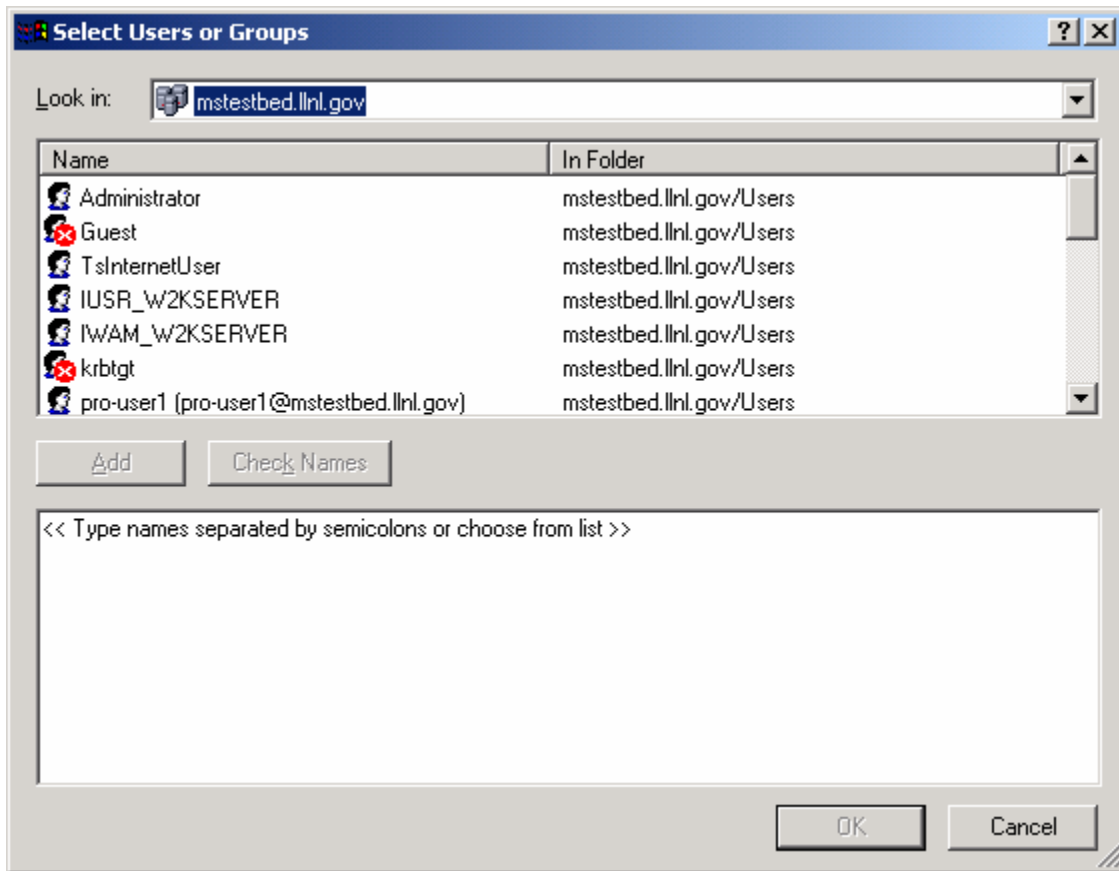
1. Right click on the **My Computer** icon on your desktop and select the **Manage** menu option.



2. Left click on the plus sign next to **Local Users and Groups** folder under the **System Tools** folder to expand it.
3. Double left click on the **Groups** folder to open it.
4. Double left click on the **Administrators** icon to open it.



5. Left click on the *Add...* button to add the user or user group to the *Administrator* group on this local computer.



6. To select a user or user groups from a domain, such as our *SafePatch Administrator* group in our previous example, choose the domain from the **Look in:** drop down list box at the top of the panel.
7. Add the user or user groups that you want and click on the **OK** button on the bottom of the panel to complete the operation.

Appendix C SafePatch Command Line

The following describes the command line syntax for SafePatch for Windows.

Usage: `java ciac.safepatch.SafePatch <options>`

Where possible options include:

<code>-?</code>	Display the help message.
<code>-h</code>	Display the help message.
<code>-ll <log level></code>	Set the logging level. ¹ <log level> is the log level <ul style="list-style-type: none">• OFF• SEVERE• WARNING• INFO• CONFIG• FINE• FINER• FINEST• ALL
<code>-id <installation directory></code>	Set the installation directory. <installation directory> is the directory where the SafePatch software is installed. ¹
<code>-c</code>	Use the color user interface. ¹
<code>-b</code>	Use the black and white user interface. ¹
<code>-v</code>	Display the SafePatch version number.
<code>-r</code>	Resets SafePatch, if SafePatch incorrectly thinks there is another instance of SafePatch already running. This can occur if SafePatch is stopped abnormally, like loss of power to the computer.
<code>-q</code>	Quiet mode. Does not play sound files. This is the default. ¹
<code>-s</code>	Play sound files. ¹

Example:

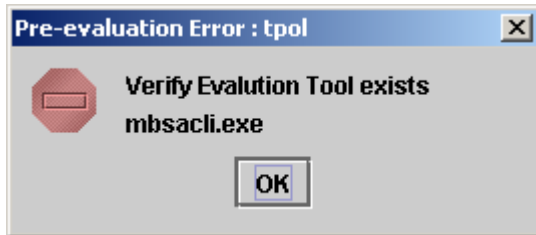
```
java ciac.safepatch.SafePatch -c -ll WARNING -id "c:\SafePatch"
```

¹ Options persist between runs and therefore only need to be set once, unless at some point you to choose to change them.

Appendix D Troubleshooting

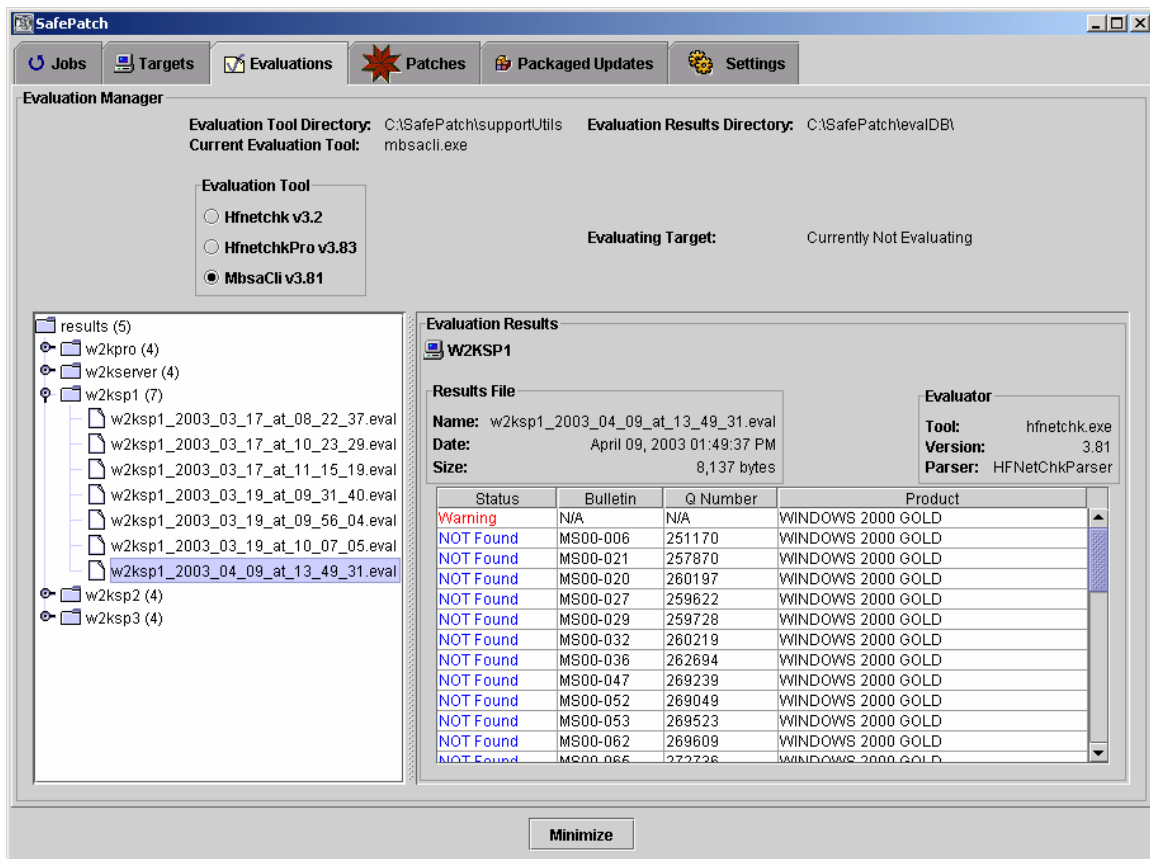
Here are a list of common problems and their solutions.

D.1 Verify Evaluation Tool Exists



Problem: When I start a target job I get an error dialog box that reads, “Verify Evaluation Tool exists.”

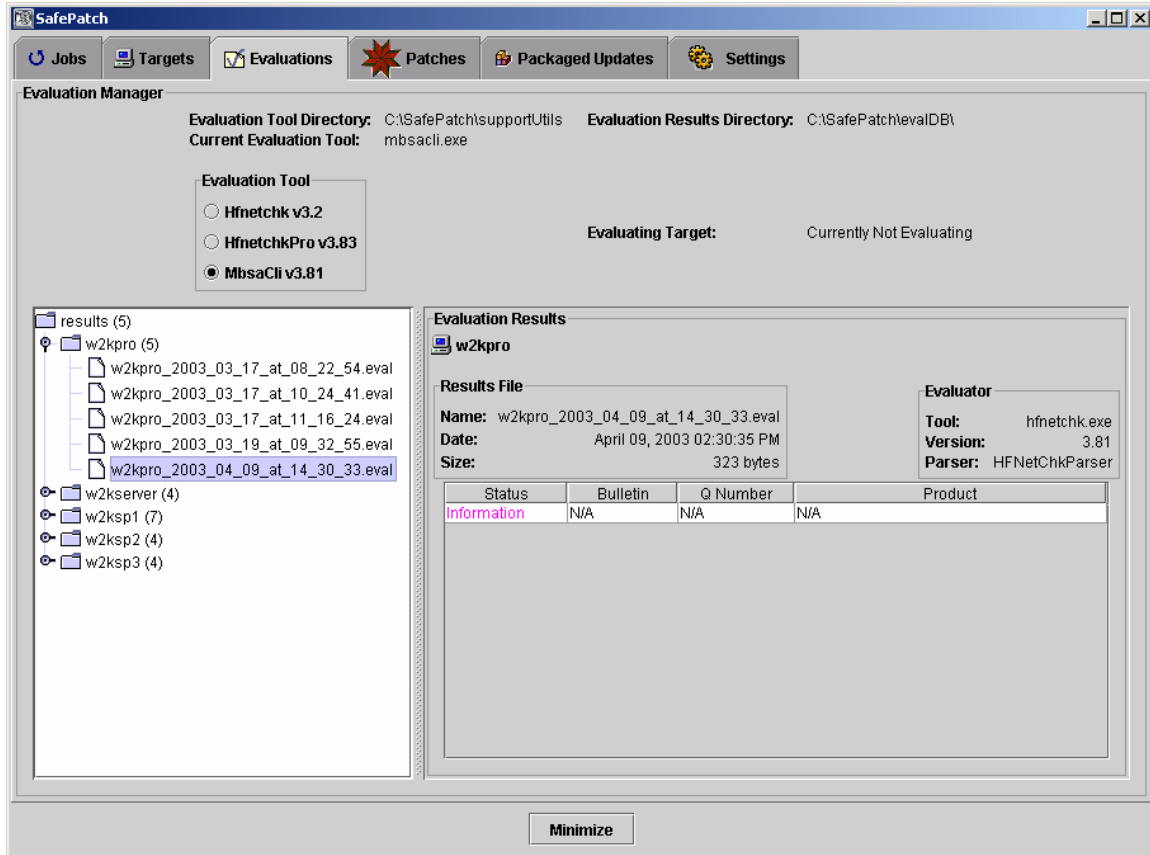
This message results from the fact that you do not have the evaluation tool selected on the **Evaluations** tabbed panel installed in the **Evaluation Tool Directory**. You must either select a tool that you have installed or install the appropriate tool. The tool is selected using the radio buttons in the **Evaluation Tool** section of the **Evaluations** tabbed panel. See 2.1 *Installing SafePatch for Windows* for instructions on installing the evaluation tool.



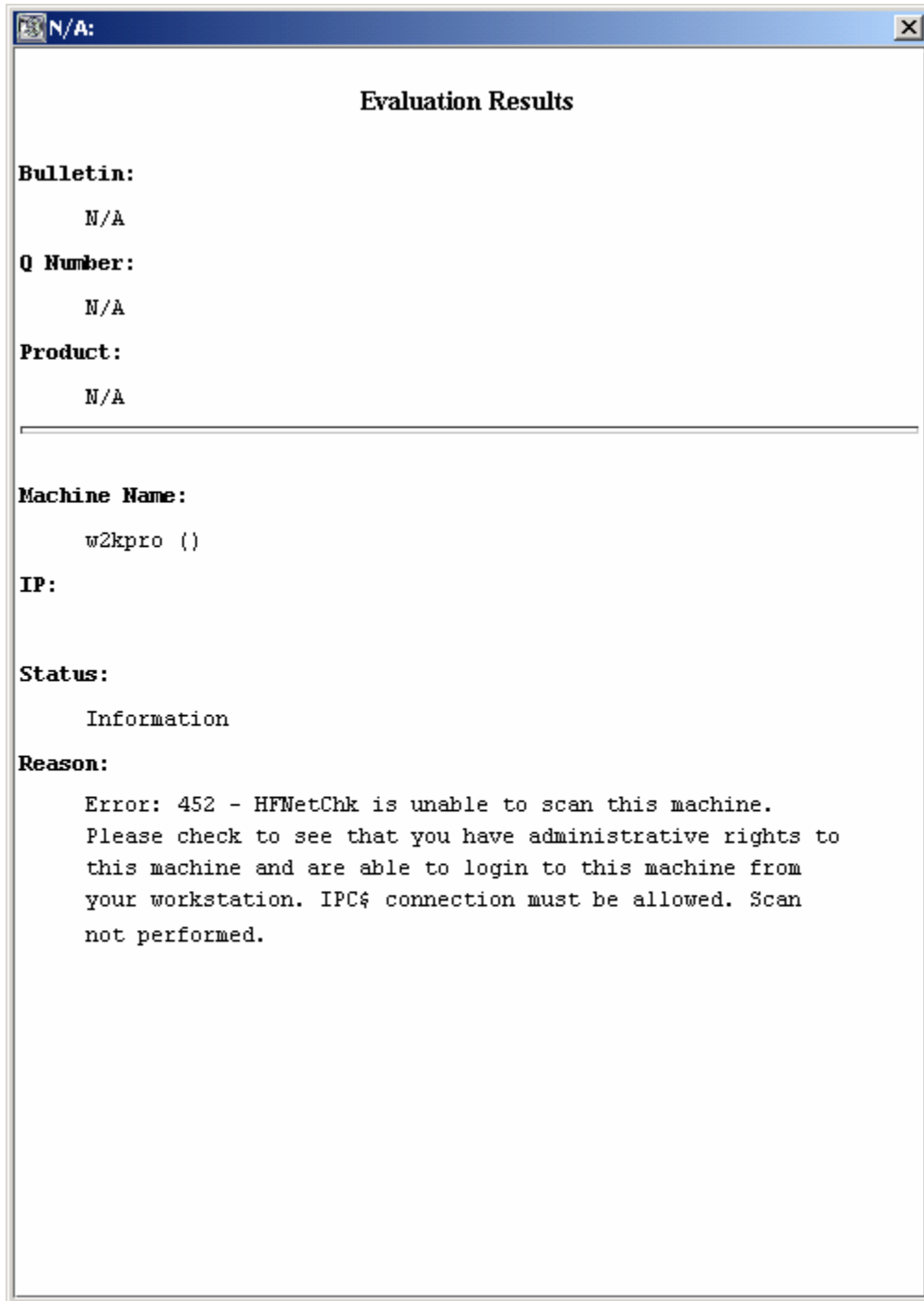
D.2 Error Creating the Target Package

Problem: In the status column on the **Jobs** tabbed panel, it reads “Error creating the Target package.”

If you get this error, most likely there was a problem communicating and evaluating the target computer or computers associated with the target job. Select the **Evaluations** tabbed panel and then the folder in the results tree corresponding to the target computer the target job was trying to evaluate. Select the appropriate report based on the date the target job ran. Click on the row in the right split pane that has a status of **Information**. A description of the cause for the failure will appear in the **Reason** section of the window.



One common reason is ***Error: Admin rights are required to scan.*** This results from not having administrator privileges on the target computer (see Appendix B *Administrator Privileges*). Another common error message states that the system or machine was not found. This typically is the result of one of two things: the target computer is not accessible on the net (e.g. it was disconnected, the computer has been shutdown etc.) or the target computer specified is not a Microsoft Windows™ computer.



N/A:

Evaluation Results

Bulletin:
N/A

Q Number:
N/A

Product:
N/A

Machine Name:
w2kpro ()

IP:

Status:
Information

Reason:
Error: 452 - HFNetChk is unable to scan this machine.
Please check to see that you have administrative rights to
this machine and are able to login to this machine from
your workstation. IPC\$ connection must be allowed. Scan
not performed.

D.3 *** Second instance of Safepatch NOT ALLOWED ***

Problem: When I start SafePatch I get the following error dialog box:



SafePatch will only allow one version of SafePatch to run at a time. You can use the Windows™ *Task Manager* to determine if another version of SafePatch is running. To start the *Task Manager*, press the **Ctrl**, **Alt** and **Delete** keys simultaneously and select the **Task Manager** button. Choose the **Applications** tabbed panel to determine if another version of SafePatch is running.

If you are sure there is not another instance of SafePatch running, you can force it to start up using a Windows™ command prompt window specifying the **-r** flag on the SafePatch command line (see Appendix C *SafePatch Command Line*) or left click the **Continue Anyway** button. SafePatch can incorrectly think that another instance is running if SafePatch was stopped abnormally, like loss of power to the computer.

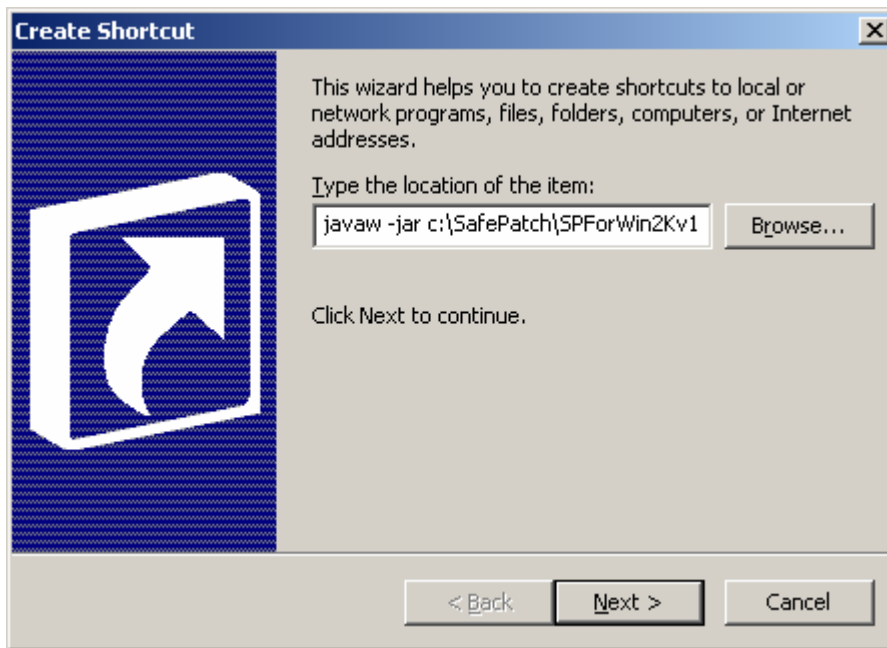
D.4 The SafePatch User Interface Is Not Responding

Problem: SafePatch appears to be hung. The user interface is not responding to my keyboard and mouse inputs.

This is most likely caused by the Windows™ command prompt window waiting for some user interaction. It is easy to inadvertently do something in the command prompt window from which SafePatch is running that will cause the command prompt window to wait for user input. An example of this occurs when you select text in the command prompt window; the command prompt window will wait for you to copy the text for use in a cut and paste operation. This will cause all other operations in the command prompt window to halt, including SafePatch. To correct this problem, select the command prompt window with your mouse and then press the **Enter** key. To avoid this in the future, it is recommended that you minimize the command prompt window, which greatly reduces the possibility of this happening.

You can also create a Windows™ shortcut for SafePatch for Windows that allows the program to be run without starting a command prompt window. This is the preferred method of using SafePatch. The batch file is useful for diagnosing problems with SafePatch for Windows by allowing you to see logging messages displayed in the command prompt window. Normally it is not necessary to see these diagnostic messages.

To create the shortcut, right click on your computer desktop. Select the *New* menu option and then the *Shortcut* item. In the text entry box type `javaw -jar c:\SafePatch\SPForWin2Kv1Jar.jar`.



You can now double click on this shortcut to start SafePatch for Windows.

D.5 The Patches Do Not Seem To Be Installing

Problem: When the installation batch file is run, it does not appear that the patches are being installed.

There are multiple ways you can run a batch file in Windows™. The method we recommend, because it gives you the most diagnostic information and control, is to start a Windows™ **Command Prompt** window, change to the directory where you unzipped the update package zip file, and type the name of the installation batch file followed by pressing the **Enter** key to execute the batch file. Most of the patches should install correctly. Some of the patches do not support the standard command line options that SafePatch uses. If you see an error regarding one or more of the patches not understanding the command line options, you should execute the patches again, either without any options or by using the **?** option to discover what options are supported. You can execute these patches either at the command line or by editing the batch file to do these patches with the appropriate command line options. See Appendix F *Patch Information*.

The second way you can execute the installation batch file is to double click on the batch file from Windows Explorer™. Using this method the batch file will run and will prompt you to press a key at the end of the batch file, so you can see the commands executed in the **Command Prompt** window. After you press a key, the **Command Prompt** window will close.

The final method of executing the installation batch file is from the *ReadMe.html* file. If you double click on the *ReadMe.html* file in Windows Explorer™, your default browser will display the file. From this display there is a link to the installation batch file. Clicking on this link will cause the batch file to execute. The problem is that many browsers change the default directory, so the batch file can no longer find the files it needs to execute. One way to solve this problem is to include the directory where you unzip the update packages in your system path.

Appendix E Support Utilities

Using Wget.exe

GNU Wget is a free software package for retrieving files using HTTP, HTTPS and FTP, the two most widely-used Internet protocols. It is a non-interactive command-line tool, so it may easily be called from scripts, cron jobs, and wrapped within other applications. SafePatch includes version 1.6 of wget with its distribution (including cygintl.dll and cygwin1.dll), as well as its accompanying documentation. Although untested with SafePatch, the most recent version of wget is 1.8.2 which supports secure socket layer. The wget web site is <http://wget.sunsite.dk>, and the executables can be directly obtained at <ftp://ftp.sunsite.dk/projects/wget/windows/wget-1.8.2b.zip> and <ftp://ftp.sunsite.dk/projects/wget/windows/ssllibs.zip>

Using Qchain.exe

Hotfix chaining during update installations is supported in Windows 2000. Qchain.exe is a utility that enables you to install multiple hotfixes without having to restart your computer after each one is installed. If multiple hotfixes replace the same file, Qchain.exe ensures that the correct version is installed. Windows 2000 SP3 and all post-SP3 hotfixes have Qchain.exe functionality built in. You can install SP3 and then install any number of post-SP3 hotfixes without having to restart the computer in between. More information about QCHAIN can be obtained from the following web site; <http://support.microsoft.com/?kbid=296861> and the tool can be downloaded directly from http://download.microsoft.com/download/9/5/2/952ac356-53cb-43a2-9c85-54b1262fca2c/Q815062_W2K_spl_X86_EN.exe

Using Extract.exe

This command-line tool extracts individual files from compressed cabinet (.cab) files. Using cabinet files is a highly efficient method of compression and distribution that has been used by Microsoft for many years. It is now available to anyone who needs to compress and distribute multiple files.

The cabinet file format is a nonproprietary format based on Lempel-Ziv compression. More information about EXTRACT can be obtained from the following web site; <http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/extract-o.asp> and the tool can be downloaded directly from http://download.microsoft.com/download/win2000platform/extract/1.00.0.1/nt5/en-us/extract_setup.exe

Using HFNetChk.exe

HFNetChk.exe is the multi-threaded command-line tool you can use to assess a computer or selected group of computers for the absence of security patches. You can use HFNetChk to assess patch status for the Windows NT 4.0, Windows NT Terminal Server, Windows 2000, Windows XP operating systems, as well as hotfixes and service packs for IIS 4.0, IIS 5.0, SQL Server 7.0, SQL Server 2000 (including MSDE), Exchange Server 5.5, Exchange Server 2000, Windows Media Player, Front Page Server Extensions, Microsoft Java Virtual Machine, Microsoft Data Access Components (MDAC), and Internet Explorer 5.01 or later.

You can download the latest version of the tool directly from Shavlik at, http://hfnetchk.shavlik.com/hfnetchk_3.86.0.1.exe

Scanning Pre-Requisites

Make sure that you meet the following requirements to make sure Hfnetchk scans successfully.

When you scan your **local** computer:

- You have administrative credentials on your local computer.
- The computer can download the patch database XML file from the Internet or obtain the file from another specified location (either on the local computer, or from a specified network location).
- The local computer is running the *Workstation* service.

NOTE: You do not have to use the Server service on the local computer.

When you scan a **remote** computer:

- You must meet all the requirements for a local scan.
- You have administrative credentials on the remote computer and can log on to the remote computer from the workstation from which you perform the scan.
- You can access the *NetBIOS* (*tcp139*) or *Direct Host* (*tcp445*) ports on the remote computer.
- The remote machine is running the *Server* service.

NOTE: You do not have to use the *Workstation* service on the remote computer.

- The remote computer is running the *Remote Registry* service.
- You can access the %systemroot% share (usually C\$ or similar) on the remote computer.

Using Mbsacli.exe

Microsoft has developed the Microsoft Baseline Security Analyzer (MBSA).

Version 1.1 is the second release of MBSA and includes a graphical and command line interface that can perform **local** or **remote** scans of Windows systems. MBSA uses the [HFNetChk](#) tool technology to scan for missing security updates and service packs for Windows, IE, IIS, SQL, Exchange, and Windows Media Player.

More information about MBSA can be obtained at the following web site, <http://support.microsoft.com/?kbid=303215#2> and the tool can be downloaded directly from; <http://download.microsoft.com/download/e/5/7/e57f498f-2468-4905-aa5f-369252f8b15c/mbsasetup.msi>

Appendix F Patch Information

At the date this document was composed, Microsoft™ employs three different methods for installing patches. The three methods are *windows script*, *update* and *hotfix*. By default SafePatch uses the command line options that are compatible with the *update* and *hotfix* patches. Using these command line options as the default works in most cases. The command line options are displayed below.

